

REMARKS

[0001] Applicant respectfully requests entry of the following remarks and reconsideration of the subject application. Applicant respectfully requests entry of the amendments herein. The remarks and amendments should be entered under 37 CFR. § 1.116 as they place the application in better form for appeal, or for resolution on the merits.

[0002] Applicant respectfully requests reconsideration and allowance of all of the claims of the application. Claims 1, 3-5, and 7-37 are presently pending. Claims amended herein are: 1, 9, 20, 35. Claims withdrawn or cancelled herein are: 2 and 6. New claims added herein are: none.

Formal Request for an Interview

[0003] If the Examiner's reply to this communication is anything other than allowance of all pending claims, then I formally request an interview with the Examiner. I encourage the Examiner to call me—the undersigned representative for the Applicant—so that we can discuss this matter so as to resolve any outstanding issues quickly and efficiently over the phone.

[0004] Please contact me or my assistant to schedule a date and time for a telephone interview that is most convenient for both of us. While email works great for us, I welcome your call to either of us as well. Our contact information may be found on the last page of this response.

Claim Amendments

[0005] Without conceding the propriety of the rejections herein and in the interest of expediting prosecution, Applicant amends claims 1, 9, 20, 35 herein. Applicant amends claims to clarify claimed features. Also, some amendments consist of dependent claims being rolled up into the base claim. For example, as amended herein, claim 1 includes the content of both dependent claims 2 and 6.

[0006] Also, the preamble of some claims are amended to clarify their meaning and to remove a term which was introduced without an antecedent basis.

[0007] Such amendments are made to expedite prosecution and to more quickly identify allowable subject matter. Such amendments are merely intended to clarify the claimed features, and should not be construed as further limiting the claimed invention in response to the cited references.

Substantive Matters

Claim Rejections under §§ 102 and 103

[0008] Claims 1-37 are rejected under 35 U.S.C. § 102 or § 103.

[0009] The Examiner rejects claims 1-3, 6-8, 11-15, and 18-19 under §102. For the reasons set forth below, the Examiner has not shown that cited references anticipate the rejected claims.

[0010] In addition, the Examiner rejects claims 4-5, 9-10, 16-17, and 20-37 under §103. For the reasons set forth below, the Examiner has not made a prima facie case showing that the rejected claims are obvious.

[0011] Accordingly, Applicant respectfully requests that the § 102 and § 103 rejections be withdrawn and the case be passed along to issuance.

[0012] The Examiner's rejections are based upon the following references alone and in combination:

- **Tsujii:** Tsujii, Shigeo et al. "An ID-Based Cryptosystem Based on the Discrete Logarithm Problem." IEE (1989);
- **Chen:** Chen, Liwung et al. "Identity Based Authenticated Key Agreement Protocols from Pairings." Proceedings of the 16th IEEE Computer Security Foundations Workshop (2003).

Overview of the Application

[0013] Short digital signatures are used in environments with bandwidth constraints and when users manually enter signatures. The shorter a signature, the easier it is for a third party to successfully break it through cryptanalysis. The Application describes strong cryptographic techniques for increasing the security of a short signature. As described, short digital ciphers (e.g., signatures) are generated and such ciphers correspond to an input message by mapping the message to a point on an elliptic curve and then scaling this point, based upon a private key, to generate another point.

[0014] On page 15, line 20 through page 16, line 2, the Application describes one aspect like this:

Roughly speaking, the exemplary short signature generator forges short digital ciphers (i.e., signatures) by computing n discrete logs of $\alpha_i P, \dots, \alpha_r P$ base P , where n is a positive integer, P is a point on an elliptic curve and a public key, and the scaling factors α_i are an unknown private key. This adds a factor of \sqrt{n} to the security of the system (i.e. the required computational effort to break the system) without affecting the signature length.

[0015] The Application also describes techniques for verification of such generated ciphers by comparing pairing values for two pairs of points.

Cited References

[0016] The Examiner cites Tsujii as its primary references in its anticipation- and obviousness-based rejections. The Examiner cites Chen as its secondary reference in its obviousness-based rejections.

Tsujii

[0017] A secure and reliable data transmission in large networks is still one of the important issues. Tsujii discloses an ID-based cryptosystem based on the discrete logarithm, problem which uses ElGamal's public key cryptosystem.

Section II @page no. 467 explains the ElGamal's public-key cryptosystem which is as follows:

ElGamal's public-key cryptosystem {11} is as follows.

< Public-Key >

p : a large prime number,
 g : a generator of $Z_p - \{0\}$
 $z = g^t \pmod{p}$ ($0 \leq t \leq p-2$).

< Secret-Key >

s : a constant number ($0 \leq s \leq p-2$).

< Encryption >

Let m ($0 \leq m \leq p-1$) be a message to be transmitted. The sender chooses a random number r ($0 \leq r \leq p-2$) and computes the cipher text C in the following:

$$C = (c_1, c_2), \quad (1)$$

$$c_1 = g^r \pmod{p}, \quad (2)$$

$$c_2 = mz^s \pmod{p}. \quad (3)$$

< Decryption >

The receiver computes

$$\begin{aligned} (c_1)^s &= (g^r)^s \pmod{p} \\ &= (g^s)^r \pmod{p} \\ &= z^r \pmod{p} \end{aligned} \quad (4)$$

and recovers the message m by

$$\begin{aligned} m &= \{(c_i)^{-1}\}^{-1} c_2 \pmod{p} \\ &= (c')^{-1} m' \pmod{p}. \end{aligned} \quad (5)$$

The implementation of the ID-based cryptosystem involves certain preparations for the centre and each entity. This includes generating the centre's secret information and each entity's secret key. (Tsuji- section III) For centre's secret information, the centre itself chooses an arbitrary large primary number p , e.g., $|p| = 512$ ($|p|$ denotes the number of bits in the binary representation for p), and also generates an n -dimensional vector a over Z_{p-1} which satisfies the following:

$$a = (a_1, a_2, \dots, a_n), \quad (8)$$

$$1 \leq a_i \leq p-2 \quad (1 \leq i \leq n), \quad (9)$$

$$a \cdot I \neq a \cdot J \pmod{p-1}, \quad I \neq J. \quad (10)$$

I, J : n -dimensional binary vectors,

and stores it as the centre's secret information.

Each entity i 's secret key s_i is produced by an inner product of a (the centre's secret information) and EID_i (the entity i 's extended id).

$$\begin{aligned} s_i &= a \cdot EID_i \pmod{p-1} \\ &= \sum_{1 \leq j \leq n} a_j y_{ij} \pmod{p-1}. \end{aligned} \quad (16)$$

An arbitrary entity's secret key, e.g., an entity k 's secret key s_k , can be decided by computing $s'_k = EID_k \cdot a \pmod{q}$. Here, a is not necessarily identical to the original entity k 's secret key s_k . The difference between s'_k and s_k is some integral multiple of q . Hence, the original entity k 's secret key s_k can be computed in at the most c trials where $p-1 = 2^c \cdot q$ and $c \ll |p|$.

Section B @page 471 of the reference talks about the enhancement of the security and the processing cost for the system. The centre partitions a 512-dimensional binary vector B into 256 segments, every two bits such as

$$B = \{b_1, b_2, b_3, b_4, \dots, b_{311}, b_{312}\} \\ = \{seg_1, seg_2, \dots, seg_{256}\}. \quad (53)$$

Then, the center defines $a(i; jk)$ ($1 \leq i \leq 256$; $j, k \in \{0, 1\}$) appropriately, computes $h(i; jk)$ ($1 \leq i \leq 256$; $j, k \in \{0, 1\}$),

$$h(i; jk) = g^{a(i; jk)} \pmod{p}, \quad (54)$$

for each seg_i , and publishes the table including every $h(i; jk)$ to all entities. Furthermore, the center computes each entity's secret key s_k by

$$s_k = \sum_{1 \leq i \leq 256} a(i; seg_{ki}) \pmod{p-1}, \quad (55)$$

depending on the entity k 's extended identity, EID_k , where EID_k is partitioned into 256 segments, every two bits, such as $EID_k = (seg_{k1}, seg_{k2}, \dots, seg_{k256})$. Then, the center distributes it to each entity through a highly secure channel. Table I gives an example of $h(i; jk)$.

TABLE I
EXAMPLE ON $h(i; jk)$

$h(1; 00) = 5$	$h(2; 00) = 21$	$h(3; 00) = 4$	$h(4; 00) = 16$
$h(1; 01) = 13$	$h(2; 01) = 17$	$h(3; 01) = 23$	$h(4; 01) = 2$
$h(1; 10) = 12$	$h(2; 10) = 7$	$h(3; 10) = 15$	$h(4; 10) = 8$
$h(1; 11) = 9$	$h(2; 11) = 11$	$h(3; 11) = 18$	$h(4; 11) = 22$

Chen

[0018] Chen's paper investigates issues related to identity based authentication key agreement protocols in the Diffie-Hellman family enabled by the Weil or Tate pairings. Such issues include how to make protocols efficient, avoiding key escrow by a trust authority (TA) that issues identity based private keys for users, and to allow users to use different TAs.

[0019] Paragraph 1 at page 3 talks about two groups G_1 and G_2 of primary order q . G_1 , with an additive notation, denotes the group of points on an elliptic curve; and G_2 , with a multiplicative notation, denotes a subgroup of the

multiplicative group of finite field. A pairing is a computational bilinear map between these two groups.

Anticipation Rejections

[0020] Applicant submits that the anticipation rejections are not valid because, for each rejected claim, no single reference discloses each and every element of that rejected claim.¹ Furthermore, the elements disclosed in the single reference are not arranged in the manner recited by each rejected claim.²

Based upon Tsujii

[0021] The Examiner rejects claims 1-3, 6-8, 11-15, and 18-19 under 35 U.S.C. § 102(b) as being anticipated by Tsujii. Applicant respectfully traverses the rejections of these claims. Based on the reasons given below, Applicant asks the Examiner to withdraw the rejection of these claims.

¹ "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987); also see MPEP §2131.

² See *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

Independent Claim 1

[0022] The Examiner indicates (Action, p. 2) the following with regard to this claim:

Regarding Claim 1, 13, Tsujii discloses the obtaining message M see Page 467- 11. El Gamal's Public-Key Cryptosystem-<Encryption>; defining a vector to v_1, \dots, v_n based upon a predefined first hashing function of the message see Page 468 -(12); calculating a private key α in accordance with equation $\sum_{i=1 \leq i \leq n} v_i \alpha \text{ mod } m$ see Page 468 item 16; producing a signature S in accordance with the equation $S = \alpha H_2(M)$, where $H_2(M)$ is a predefined second hashing function see Page 470-(39).

[0023] As previous written, claims 1 and 13 cover similar content, but different statutory subject matter. However, claim 1 is amended and now differs from claim 13. In particular, the amendments include clarification of some aspects and inclusion of the content of both dependent claims 2 and 6.

[0024] Applicant submits that Tsujii does not anticipate this claim because it does not show or disclose, at least, the following features as recited in this claim (with emphasis added):

- defining a vector v to be v_1, \dots, v_n based upon a predefined first hashing function of the message M ;
- calculating a private key α [alpha] in accordance with this equation $\alpha = \sum_{i=1}^n v_i \alpha_i \text{ mod } m$, where m is an order of torsion points;
- producing a signature S in accordance with this equation: $S = \alpha H_2(M)$, where $H_2(M)$ is a predefined second hashing function of the message M , wherein the predefined first hashing function differs from the predefined second hashing function and wherein the signature S is represented by a number of bits;
- truncating a specific number of bits off of signature S ;
- after the truncating, indicating a message-and-signature pair (M, S) based, at least in part, on the obtaining, defining, calculating, or producing

[0025] Instead of disclosing “defining a vector v to be v_1, \dots, v_n based upon a predefined first hashing function of the message,” Tsujii shows computing of its vector a as a function of w and p , where neither w nor p is “the message,” as recited in the claim as being the basis for defining the vector. The following selected portions for Tsujii supports the Applicant’s position:

The center also chooses a w which satisfies $\text{GCD}(w, p - 1) = 1$ and computes an n -dimensional vector a as follows:

$$a_i = a_i' w \pmod{p - 1} \quad (1 \leq i \leq n), \quad (12)$$

$$a = (a_1, a_2, \dots, a_n). \quad (13)$$

(Tsujii, p. 468, regarding equations (12) and (13))

< Public-Key >

p : a large prime number,

g : a generator of $Z_p - \{0\}$

$z = g^s \pmod{p} \ (0 \leq s \leq p - 2).$

(Tsuji, p. 467, under "<Public-Key> heading)

[0026] Notice that w is a value that "satisfies $\text{GCD}(w, p-1) = 1$ and that p is a "large prime number." Notice neither one of them are the message of Tsujii defined under the "<Encryption>" heading on p. 467:

Let $m(0 \leq m \leq p - 1)$ be a message to be transmitted. The sender chooses a random number $r(0 \leq r \leq p - 2)$ and computes the cipher text C in the following:

Consequently, Tsujii fails to disclose, "defining a vector v to be v_1, \dots, v_n **based upon a predefined first hashing function of the message,**" as recited in the claim.

[0027] Furthermore, instead of disclosing "calculating a private key α [alpha] in accordance with this equation $\alpha = \sum_{i=1}^n v_i \alpha_i \pmod{m}$," Tsujii shows a calculation of a secret key s_j by a function of γ and p , where neither γ nor p is alpha nor the message (M), as recited in the claim as being the part of the claimed equation. Moreover, Tsujii fails to disclose use of m , where " m is an order of torsion points," as recited in the claim.

[0028] The following selected portions for Tsujii supports the Applicant's position:

Step 5—Each Entity's Secret Key: The center computes the entity i 's secret key s_i by the inner product of a (the center's secret information) and EID_i [the entity i 's extended ID; see (7)].

$$\begin{aligned} s_i &= a \cdot EID_i \pmod{p-1} \\ &= \sum_{1 \leq j \leq n} a_j y_{ij} \pmod{p-1}. \end{aligned} \quad (16)$$

(Tsujii, p. 468, regarding equation (16))

< Public-Key >

p : a large prime number,
 g : a generator of $Z_p - \{0\}$
 $z = g^s \pmod{p} \ (0 \leq s \leq p-2).$

(Tsujii, p. 467, under "<Public-Key> heading)

[0029] Accordingly, Tsujii fails to disclose "defining a vector v to be v_1, \dots, v_n based upon a predefined first hashing function of the message."

[0030] Furthermore, instead of disclosing "producing a signature S in accordance with this equation: $S = aH2(M)$, where $H2(M)$ is a predefined second hashing function **of the message**," Tsujii shows a computation based upon the "Carmichael function of N " (see M.R. Schroeder, "Number theory in science and communication," Springer Series in Information Sciences, 1986).

[0031] The following selected portions for Tsujii supports the Applicant's position:

Since each EID_i is an n -dimensional binary vector, there exists an $(n + 1)$ -dimensional vector c over the integer ring such that

$$\sum_{1 \leq i \leq n+1} c_i EID_i = 0. \quad (37)$$

Here, we have

$$\sum_{1 \leq i \leq n+1} c_i s_i = 0 \pmod{\lambda(N)}, \quad (38)$$

and thus,

$$\sum_{1 \leq i \leq n+1} c_i s_i = A\lambda(N). \quad (39)$$

If $A \neq 0$, the $(n + 1)$ entities can have an integer multiple of $\lambda(N)$, and they can find the factorization of N [18]. Then, a similar method with Attack 1 is applicable; hence, the center's secret information can be derived by $(n + 1)$ entities' conspiracy. \square

(Tsujii, p. 469, equation (39) is what the Examiner indicates discloses this feature of the claims)

By this minor change, the system in Section III is slightly modified such that $(p - 1)$ is replaced by $\lambda(N)$ where $\lambda(N)$ is the Carmichael function of N [16] and g , a generator in $Z_p - \{0\}$, is replaced by g' , a generator of the multiplicative group in Z_N . For the modified system. Cop-

(Tsujii, p. 470, under "Modified System and Security" heading)

[0032] This equation (39) cited by the Examiner is not a “hashing function **of the message.**” Consequently, Tsujii fails to disclose “producing a signature S in accordance with this equation: $S = \alpha H_2(M)$, where $H_2(M)$ is a predefined second hashing function **of the message**”

[0033] Further still, the Examiner has not shown where the reference shows (as recited in the claim):

- “the predefined first hashing function [being different] from the predefined second hashing function”
- “truncating a specific number of bits off of signature S” and doing so next “indicating”
- “indicating a message-and-signature pair (M, S)”

[0034] Accordingly, Tsujii does not disclose all of the claimed elements and features of this claim. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Dependent Claims 2-8

[0035] Claims 2 and 6 are canceled because their content is now rolled up into claim 1, as amended.

[0036] For the remaining claims, these claims ultimately depend upon independent claim 1. As discussed above, claim 1 is allowable. It is axiomatic that any dependent claim, which depends from an allowable base claim, is also

allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

Independent Claim 13

[0037] The Examiner indicates (Action, p. 2) the following with regard to this claim:

Regarding Claim 1, 13, Tsujii discloses the obtaining message M see Page 467- 11. El Gamal's Public-Key Cryptosystem-<Encryption>; defining a vector to v_1, \dots, v_n based upon a predefined first hashing function of the message see Page 468 -(12); calculating a private key α in accordance with equation $\sum_{i=1}^n v_i \alpha_i \bmod m$ see Page 468 item 16; producing a signature S in accordance with the equation $S = \alpha \cdot H_2(M)$, where $H_2(M)$ is a predefined second hashing function see Page 470-(39).

[0038] Applicant submits that Tsujii does not anticipate this claim because it does not show or disclose, at least, the following features as recited in this claim (with emphasis added):

- defining a vector v to be v_1, \dots, v_n **based upon a predefined first hashing function of the message;**
- calculating a private key a [alpha] **in accordance with this equation** $\alpha = \sum_{i=1}^n v_i \alpha_i \bmod m$;
- producing a signature S in accordance with this equation: $S = aH_2(M)$, where $H_2(M)$ is a predefined second hashing function **of the message**

[0039] Instead of disclosing "defining a vector v to be v_1, \dots, v_n **based upon a predefined first hashing function of the message,**" Tsujii shows computing of its vector a as a function of w and p , where neither w nor p is "the message," as recited in the claim as being the basis for defining the vector. The following selected portions for Tsujii supports the Applicant's position:

The center also chooses a w which satisfies $\text{GCD}(w, p - 1) = 1$ and computes an n -dimensional vector a as follows:

$$a_i = a'_i w \pmod{p - 1} \quad (1 \leq i \leq n), \quad (12)$$

$$a = (a_1, a_2, \dots, a_n). \quad (13)$$

(Tsujii, p. 468, regarding equations (12) and (13))

< Public-Key >

p : a large prime number,

g : a generator of $Z_p - \{0\}$

$z = g^x \pmod{p} \quad (0 \leq x \leq p - 2).$

(Tsujii, p. 467, under "<Public-Key> heading)

[0040] Notice that w is a value that "satisfies $\text{GCD}(w, p-1) = 1$ and that p is a "large prime number." Notice neither one of them are the message of Tsujii defined under the "<Encryption>" heading on p. 467:

Let $m(0 \leq m \leq p - 1)$ be a message to be transmitted. The sender chooses a random number $r(0 \leq r \leq p - 2)$ and computes the cipher text C in the following:

Consequently, Tsujii fails to disclose, "defining a vector v to be v_1, \dots, v_n **based upon a predefined first hashing function of the message.**"

[0041] Furthermore, instead of disclosing "calculating a private key α [alpha] in accordance with this equation $\alpha = \sum_{i=1}^n v_i \alpha_i \text{ mod } m$," Tsujii shows a calculation of a secret key s_i by a function of y and p , where neither y nor p is a nor the message (M), as recited in the claim as being the part of the claimed equation.

[0042] The following selected portions for Tsujii supports the Applicant's position:

Step 5—Each Entity's Secret Key: The center computes the entity i 's secret key s_i by the inner product of a (the center's secret information) and EID_i [the entity i 's extended ID; see (7)].

$$\begin{aligned} s_i &= a \cdot \text{EID}_i \pmod{p-1} \\ &= \sum_{1 \leq j \leq n} a_j y_{ij} \pmod{p-1}. \end{aligned} \quad (16)$$

(Tsuji, p. 468, regarding equation (16))

< Public-Key >

p : a large prime number,

g : a generator of $Z_p - \{0\}$

$z = g^s \pmod{p} \ (0 \leq s \leq p - 2).$

(Tsuji, p. 467, under "<Public-Key> heading)

[0043] Accordingly, Tsuji fails to disclose "defining a vector v to be v_1, \dots, v_n based upon a predefined first hashing function of the message."

[0044] Furthermore, instead of disclosing "producing a signature S in accordance with this equation: $S = aH2(M)$, where $H2(M)$ is a predefined second hashing function of the message," Tsuji shows a computation based upon the "Carmichael function of N " (see M.R. Schroeder, "Number theory in science and communication," Springer Series in Information Sciences, 1986).

[0045] The following selected portions for Tsuji supports the Applicant's position:

Since each EID_i is an n -dimensional binary vector, there exists an $(n + 1)$ -dimensional vector c over the integer ring such that

$$\sum_{1 \leq i \leq n+1} c_i \text{EID}_i = 0. \quad (37)$$

Here, we have

$$\sum_{1 \leq i \leq n+1} c_i x_i = 0 \pmod{\lambda(N)}, \quad (38)$$

and thus,

$$\sum_{1 \leq i \leq n+1} c_i x_i = A\lambda(N). \quad (39)$$

If $A \neq 0$, the $(n + 1)$ entities can have an integer multiple of $\lambda(N)$, and they can find the factorization of N [18]. Then, a similar method with Attack 1 is applicable; hence, the center's secret information can be derived by $(n + 1)$ entities' conspiracy. \square

(Tsujii, p. 469, equation (39) is what the Examiner indicates discloses this feature of the claim)

By this minor change, the system in Section III is slightly modified such that $(p - 1)$ is replaced by $\lambda(N)$ where $\lambda(N)$ is the Carmichael function of N [16] and g , a generator in $\mathbb{Z}_p - \{0\}$, is replaced by g' , a generator of the multiplicative group in \mathbb{Z}_N . For the modified system. Con-

(Tsujii, p. 470, under "Modified System and Security" heading)

[0046] This equation (39) cited by the Examiner is not a "hashing function of the message." Consequently, Tsujii fails to disclose "producing a signature S

in accordance with this equation: $S = \alpha H_2(M)$, where $H_2(M)$ is a predefined second hashing function **of the message**”

[0047] Accordingly, Tsujii does not disclose all of the claimed elements and features of this claim. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Dependent Claims 14-19

[0048] These claims ultimately depend upon independent claim 13. As discussed above, claim 13 is allowable. It is axiomatic that any dependent claim, which depends from an allowable base claim, is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

Dependent Claims 11-12

[0049] According to the Action, claims 11 and 12 are rejected based upon anticipation (i.e., § 102). However, claims 11 and 12 are dependent claims, which depend from independent claim 9. According to this Action, claim 9 is rejected as being unpatenable under § 103 (i.e., obvious) based upon a combination of references.

[0050] Applicant is unsure how dependent claims, which are presumptively narrower than independent claim, would be rejected as being anticipated by one

reference while their base independent claim is rejected as being obvious based upon a combination of references.

[0051] In this confusion, Applicant will treat claims 11-12 as being rejected as being obvious based upon the same combination of references as its base independent claim (claim 9).

Obviousness Rejections

Lack of *Prima Facie* Case of Obviousness (MPEP § 2142)

[0052] Applicant disagrees with the Examiner's obviousness rejections. Arguments presented herein point to various aspects of the record to demonstrate that not all of the criteria set forth for making a prima facie case have been met.

Based upon Tsujii and Chen

[0053] The Examiner rejects claims 4-5, 9-10, 16-17, and 20-37 under 35 U.S.C. § 103(a) as being unpatentable over Tsujii in view of Chen. Applicant respectfully traverses the rejection of these claims and asks the Examiner to withdraw the rejection of these claims.

[0054] Claims 4-5 and 16-17 ultimately depend upon independent claims 1 and 13. As discussed above, claims 1 and 13 are allowable. It is axiomatic that any dependent claim, which depends from an allowable base claim, is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

Claim 4-5, 9-10, 16-17, 22, and 30

[0055] One pp. 2-4 of the Action, the Examiner offers a blanket rejection of claims 4-5, 9-10, 16-17, 22, and 30 (of which claim 9 is on the only independent claim). The following is the complete text of the Examiners rejection of these claims:

Regarding Claim 4-5, 9-10,16-17, 22, 30,Tsujii disclose the discrete logs of points on an elliptic curve and tate-weil pairings. However, Chen discloses the discrete logs of points on an elliptic curve and tate-weil pairings see Page 9 14¶ “Suppose that there are...”.

[0056] Applicant submits that this rejection is confusing and lacking in support.

[0057] Initially, the Examiner says that Tsujii discloses “the discrete logs of points on elliptic curve and tate-weil pairing.” However, the Examiner provides support for this assertion. No portion or section of Tsujii is pointed towards as supporting the Examiner’s assertion. Therefore, the Applicant respectfully requests that next Action—which is expected to be non-Final—provide support for this assertion.

[0058] Next, the Examiner says that Chen also discloses “the discrete logs of points on elliptic curve and tate-weil pairing.” It is unclear as to why the Examiner relies upon both references for suggesting and teaching the same information. Perhaps, the Examiner meant that Tsujii did NOT disclose it but Chen did.

[0059] To support the assertion that Chen discloses the claim language, the Examiner points to "Page 9 14¶ "Suppose that there are...", presumably of Chen. This is what that paragraph says:

Suppose that there are two trusted authorities, say TA_1 and TA_2 ; they each have a public/private key pair: $(P, s_1P \in G_1, s_1 \in \mathbb{Z}_q^*)$ and $(P, s_2P \in G_1, s_2 \in \mathbb{Z}_q^*)$, where P and G_1 are globally agreed, e.g., recommended by an international standard body.

[0060] Applicant is at a lost at understanding how the Examiner sees the claim language of claims 4-5, 9-10, 16-17, 22, and 30 in the above paragraph of Chen. For the reader to better compare the cited language of Chen, here is the claim language of some of the claims being rejected based upon Chen:

9. A computer-readable medium ... comprising:
choosing n discrete logs of $\alpha_1P, \dots, \alpha_nP$ base P , where n is a positive integer, P is a point on an elliptic curve and a public key, and α_i is a scaling factor and a private key; ...
10. A medium as recited in claim 9, wherein a point is of order and where denotes a Tate or Weil or Squared Tate or Squared Weil Pairing, where = and where q is a prime power.

[0061] Other than a few minor superficial terms (e.g., P , public key, private key), The Examiner has not identified where any cited reference discloses anything found in these claims.

[0062] Accordingly, the Examiner has failed to establish its prima facie case for the obviousness rejection. Furthermore, the cited references (alone or in

combination) fail to disclose, teach, or suggest all of the elements/features found in these claims. Applicant asks the Examiner to withdraw the rejections.

No Reason to Combine References

[0063] Applicant submits that Examiner has not identified a valid reason that would have led one of ordinary skill in the art at the time of the invention (hereinafter, "OOSA") to combine the disclosures of the cited references in the manner claimed.

[0064] Here is the Examiner's state reason for combining the teachings of the references (p. 4 of the Action):

an elliptic curve and tate-weil pairings see Page 9 14¶ "Suppose that there are...". It would be obvious to one having ordinary skill in the art at the time of the invention to include the discrete logs of points on an elliptic curve and tate-weil pairings in the invention of Tsujii in order to unique session keys.

[0065] Applicant is unsure and unclear on how to interpret this reasoning. What does it mean to "unique session keys?" Why is that desirable? More importantly, the Examiner does not point out the source of the reasons to combine the teachings. Why would OOSA look at these two references? Why would it be logical for OOSA to look to one reference to solve the problems related to the other reference? The Examiner does not address these questions or issues.

[0066] Therefore, there is no valid reason that would have led OOSA to combine the disclosures of the cited references in the manner claimed. Accordingly, the Applicant therefore respectfully asks the Examiner to withdraw the rejection of these claims.

[0067] As shown above, the combination of Chen and Tsujii does not disclose all of the claimed elements and features of these claims. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Dependent Claims 10-12

[0068] These claims ultimately depend upon independent claim 9. As discussed above, claim 9 is allowable. It is axiomatic that any dependent claim, which depends from an allowable base claim, is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

Claim 20, 27, 28, 35, and 37

[0069] One pp. 4 of the Action, the Examiner offers a blanket rejection of claims 20, 27, 28, 35, and 37 (of which claims 20, 28, and 35 are the independent claims). The following is the complete text of the Examiner's rejection of these claims:

Regarding Claim 26, 27, 28, 35, 37, Tsujii discloses the obtaining message M and signature(M, S) see Page 471-(55) & Page 467- II. El Gamal's Public-Key Cryptosystem- <Encryption>; defining a vector to v_1, \dots, v_n based upon a predefined first hashing function of the message see Page 468 -(12); calculating a private key α in accordance with equation $Q = \sum_{i=1 \leq i \leq n} v_i Q_i \text{ mod } m$ see Page 468 item 16. But does not disclose the calculating the point on an elliptic curve, comparing of pair (P, S) and pair $(Q, H_2(M))$ and indicating results of comparing. However, Chen discloses the point on an elliptic curve (Page 3 1 ¶), comparing of pair (P, S) and pair $(Q, H_2(M))$ and indicating results of comparing see (Page 1 ¶) "At the conclusion...". It would be obvious to one having ordinary skill in the art at the time of the invention to include the calculating the point on an elliptic curve, comparing of pair (P, S) and pair $(Q, H_2(M))$ and indicating results of comparing in the invention of Tsujii in order to have an authentication system/key verification system as taught in Chen see Page 10 9 ¶ "The method used ...".

[0070] Neither reference discloses: "obtaining an input message-and-signature pair (M, S) ." The Examiner indicates that the following text from Tsujii discloses this claim language:

for each seg_i , and publishes the table including every $h(i; jk)$ to all entities. Furthermore, the center computes each entity's secret key s_k by

$$s_k = \sum_{i \leq i \leq 256} a(i; \text{seg}_{ki}) \pmod{p-1}, \quad (55)$$

depending on the entity k 's extended identity, EID_k , where EID_k is partitioned into 256 segments, every two bits, such as $\text{EID}_k = (\text{seg}_{k1}, \text{seg}_{k2}, \dots, \text{seg}_{k256})$. Then, the center distributes it to each entity through a highly secure channel. Table I gives an example of $h(i; jk)$.

[0071] Where is the "input message-and-signature pair (M,S)?" This is the text cited by the Examiner as that which discloses, teaches, or suggests the obtaining of an "input message-and-signature pair (M,S)." Applicant submits that this cited text and all of Tsujii for that matter is silent on this claimed feature.

[0072] Instead of disclosing "defining a vector v to be v_1, \dots, v_n based upon a predefined first hashing function of the message," Tsujii shows computing of its vector a as a function of w and p , where neither w nor p is "the message," as recited in the claim as being the basis for defining the vector. The following selected portions for Tsujii supports the Applicant's position:

The center also chooses a w which satisfies $\text{GCD}(w, p-1) = 1$ and computes an n -dimensional vector a as follows:

$$a_i = a_i' w \pmod{p-1} \quad (1 \leq i \leq n), \quad (12)$$

$$a = (a_1, a_2, \dots, a_n). \quad (13)$$

(Tsujii, p. 468, regarding equations (12) and (13))

< Public-Key >

p : a large prime number,
 g : a generator of $Z_p - \{0\}$
 $z = g^s \pmod{p} \ (0 \leq s \leq p - 2).$

(Tsujii, p. 467, under "<Public-Key> heading)

[0073] Notice that w is a value that "satisfies $\text{GCD}(w, p-1) = 1$ and that p is a "large prime number." Notice neither one of them are the message of Tsujii defined under the "<Encryption>" heading on p. 467:

Let $m(0 \leq m \leq p - 1)$ be a message to be transmitted. The sender chooses a random number $r(0 \leq r \leq p - 2)$ and computes the cipher text C in the following:

Consequently, Tsujii fails to disclose "defining a vector v to be v_1, \dots, v_n **based upon a predefined first hashing function of the message.**"

[0074] Furthermore, neither Chen nor Tsujii disclose:

- calculating a point Q on an elliptic curve in accordance with this equation: $Q = \sum_{i=1}^n v_i Q_i$;
- comparing pairing outputs of a pair (P, S) and a pair $(Q, H_2(M))$, where $H_2(M)$ is a predefined second hashing function of M and P is a point on the elliptic curve; [claims 20 and 28]
- comparing pairing outputs of a pair (P, S) and a pair $(Q, H_2(M))^u$, where $H_2(M)$ is a predefined second hashing function of M and P

is a point on the elliptic curve and μ is an integer in a defined range; [claim 35]

[0075] Accordingly, the Examiner has failed to establish its prima facie case for the obviousness rejection. Furthermore, the cited references (alone or in combination) fail to disclose, teach, or suggest all of the elements/features found in these claims. Applicant asks the Examiner to withdraw the rejections.

No Reason to Combine References

[0076] Applicant submits that Examiner has not identified a valid reason that would have led one of ordinary skill in the art at the time of the invention (hereinafter, "OOSA") to combine the disclosures of the cited references in the manner claimed.

[0077] Here is the Examiner's state reason for combining the teachings of the references (p. 4 of the Action):

conclusion..."). It would be obvious to one having ordinary skill in the art at the time of the invention to include the calculating the point on an elliptic curve, comparing of pair (P, S) and pair (Q, H₂(M)) and indicating results of comparing in the invention of Tsujii in order to have an authentication system/key verification system as taught in Chen see Page 10 ¶¶ "The method used ...".

[0078] Applicant submits that this reasoning is invalid on its face. Based upon the reasoning given above, it is the Examiner's position that OOSA would look towards the teaching of Tsujii "in order to have an authentication

system/key verification system as taught in Chen.” However, by the Examiner’s own admission, Chen already **has** the very system that the teaching of Tsujii somehow enables Chen to **have**. Applicant is quite confused as to how Tsujii’s teaching helps Chen possess (i.e., “have”) something that is already possesses.

[0079] Furthermore, the Examiner does not point out the source of the reasons to combine the teachings. Why would OOSA look at these two references? Why would it be logical for OOSA to look to one reference to solve the problems related to the other reference? The Examiner does not address these questions or issues.

[0080] Therefore, there is no valid reason that would have led OOSA to combine the disclosures of the cited references in the manner claimed. Accordingly, the Applicant therefore respectfully asks the Examiner to withdraw the rejection of these claims.

[0081] As shown above, the combination of Chen and Tsujii does not disclose all of the claimed elements and features of these claims. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Dependent Claims 21, 23-26, 29, 31-34, and 36

[0082] These claims ultimately depend upon independent claims 20, 28, and 35. As discussed above, claims 20, 28, and 35 are allowable. It is axiomatic that any dependent claim, which depends from an allowable base

claim, is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

Dependent Claims

[0083] In addition to its own merits, each dependent claim is allowable for the same reasons that its base claim is allowable. Applicant requests that the Examiner withdraw the rejection of each dependent claim where its base claim is allowable.

Conclusion

[0084] All pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the **Examiner is urged to contact me before issuing a subsequent Action.** Please call or email me or my assistant at your convenience.

Respectfully Submitted,

Lee & Hayes, PLLC
Representatives for Applicant

/kaseychristie40559/

Dated: 9/17/2008

Kasey C. Christie (kasey@leehayes.com; x232)

Registration No. 40559

Customer No. **22801**

Telephone: (509) 324-9256

Facsimile: (509) 323-8979

www.leehayes.com